1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

013030228 **Image available**
WPI Acc No: 2000-202079/ **200018**
XRPX Acc No: N00-150560

Authentication system of network access for mobile communication network, includes remote access processor which performs approval of access to mobile computer based on its detected positional information

Patent Assignee: NTT DATA TSUSHIN KK (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000040064	A	20000208	JP 98208818	A	1998072	200018	B

Priority Applications (No Type Date): JP 98208818 A 19980724
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000040064	A		7	G06F-015/00	

Abstract (Basic): JP 2000040064 A

NOVELTY - The correctness of access is judged based on the positional information of a mobile computer (11). Then, it is recognized whether the judged result is legitimate during access to server. The approval of access is provided by remote access processor (29) based on the recognized result.

USE - For authentication of network access by mobile computer.

ADVANTAGE - Inaccurate access to cable network from mobile computer is prevented. DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of authentication server. (11) Mobile computer; (29) Remote access processor.

Dwg.3/3

Title Terms: AUTHENTICITY; SYSTEM; NETWORK; ACCESS; MOBILE; COMMUNICATE; NETWORK; REMOTE; ACCESS; PROCESSOR; PERFORMANCE; APPROVE; ACCESS; MOBILE; COMPUTER; BASED; DETECT; POSITION; INFORMATION
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/00
International Patent Class (Additional): H04L-009/32; H04Q-007/38
File Segment: EPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06454491 **Image available**
CERTIFYING SYSTEM OF NETWORK ACCESS

PUB. NO.: 2000-040064 A]
PUBLISHED: February 08, 2000 (20000208)
INVENTOR(s): TAKAHASHI NARIFUMI
YOSHIKAWA AKIO
APPLICANT(s): NTT DATA CORP
APPL. NO.: 10-208818 [JP 98208818]
FILED: July 24, 1998 (19980724)
INTL CLASS: G06F-015/00; H04Q-007/38; H04L-009/32

ABSTRACT

PROBLEM TO BE SOLVED: To prevent illegal access in the case of accessing from a mobile terminal to a cable network.

SOLUTION: Corresponding to remote access from a mobile terminal 11 to the network, a communication processing part 23 receives an originating ID

transmitted from the mobile terminal 11 and dispatches it to an originating ID processing part 27. While using this originating ID, the originating ID processing part 27 requests the acquisition of the past access history of the mobile terminal 11 to a certified information preserving part 25 and when the past access history is received, the originating ID processing part 27 calculates the moving velocity (v) of the mobile terminal 11 from the past access history, the current positional information and the access time or the like of the mobile terminal 11 supplied from the mobile terminal 11. When the moving velocity (v) does not exceed the upper limit value of the moving velocity, the originating ID processing part 27 judges it as legal access and a remote access processing part 29 permits the access. When the moving velocity (v) exceeds the upper limit value of the moving velocity, the access at this time is judged as an illegal one and the remote access processing part 29 inhibits the access.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－40064
（P2000－40064A）
(43)公開日　平成12年２月８日(2000.2.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ	５Ｂ０８５
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｋ０１３
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ	５Ｋ０６７

審査請求　未請求　請求項の数10　ＯＬ　（全７頁）

(21)出願番号　特願平10－208818

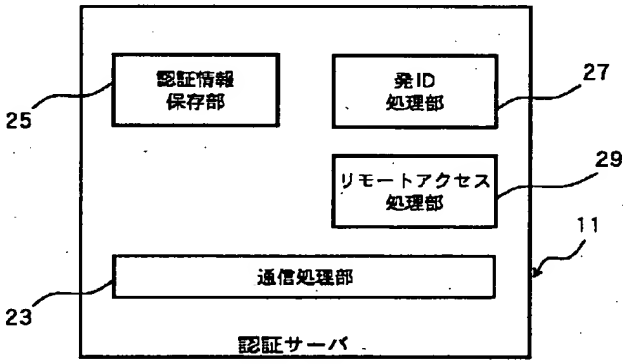
(22)出願日　平成10年７月24日(1998.7.24)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　高橋　成文
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(72)発明者　吉川　明夫
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(74)代理人　100095371
弁理士　上村　輝之

最終頁に続く

(54)【発明の名称】　ネットワークアクセスの認証方式

(57)【要約】
【課題】　移動端末から有線ネットワークへのアクセスにおいて、不正アクセスを防止できるようにする。
【解決手段】　移動端末１１のネットワーク７へのリモートアクセスにより、通信処理部２３は、移動端末１１から送信される発ＩＤを受け取り、発ＩＤ処理部２７に渡す。発ＩＤ処理部２７では、この発ＩＤを用いて移動端末１１の過去のアクセス履歴の取得要求を認証情報保存部２５に行い、過去のアクセス履歴が与えられると、発ＩＤ処理部２７では、過去のアクセス履歴と移動端末１１から与えられる移動端末１１の現在位置情報及びアクセス時刻等から、移動端末１１の移動速度ｖを求める。発ＩＤ処理部２７では、移動速度ｖが移動速度上限値を超えていなければ正当なアクセスとして、リモートアクセス処理部２９において上記アクセスが許可される。移動速度ｖが移動速度上限値を超えていれば今回のアクセスは不正アクセスであると判断して、リモートアクセス処理部２９において上記アクセスが禁止されることになる。



1

【特許請求の範囲】

【請求項１】　移動クライアントがネットワーク上のサーバから所望の情報を取得する環境において、
前記移動クライアントの前記サーバへのアクセス時に、移動クライアントからの位置情報に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可する手段を備えることを特徴とするネットワークアクセスの認証方式。

【請求項２】　移動クライアントがネットワーク上のサーバから所望の情報を取得する環境において、
前記移動クライアントの前記サーバへのアクセス時に、移動クライアントからの位置情報によりその移動速度を演算する手段と、
前記演算された移動速度に基づいて前記アクセスの正当性を判断し、正当と認めたときアクセスを許可する手段と、
を備えることを特徴とするネットワークアクセスの認証方式。

【請求項３】　請求項２記載のネットワークアクセスの認証方式において、
前記移動クライアントが、ＧＰＳ又はＰＨＳのローミング機構を用いて自身の現在位置を検出することを特徴とするネットワークアクセスの認証方式。

【請求項４】　請求項２記載のネットワークアクセスの認証方式において、
前記位置情報が、今回のアクセス時における移動クライアントの位置情報と、前回のアクセス時における移動クライアントの位置情報とを含み、
前記アクセス許可手段が、前記各位置情報から前記移動速度演算手段によって求められた移動速度が所定の移動速度上限値を超えたとき、今回のアクセスを不正アクセスと判断することを特徴とするネットワークアクセスの認証方式。

【請求項５】　請求項２記載のネットワークアクセスの認証方式において、
前記移動クライアントからのログイン名及びパスワード名と、予め蓄積されるログイン名データ及びパスワード名データとが一致するか否かを判定する手段を更に備え、
前記判定手段から一致した旨の判定結果が得られたとき、前記移動速度演算手段及び前記アクセス許可手段の処理動作が実行されることを特徴とするネットワークアクセスの認証方式。

【請求項６】　移動クライアントがネットワーク上のサーバから所望の情報を取得する環境において、
前記移動クライアントの前記サーバへのアクセス時に、移動クライアントからの位置情報により移動クライアントが所定領域内に存在するか否かを判定する手段と、
前記判定された結果に基づいて前記アクセスの正当性を判断し、正当と認めたときアクセスを許可する手段と、

2

を備えることを特徴とするネットワークアクセスの認証方式。

【請求項７】　請求項６記載のネットワークアクセスの認証方式において、
前記移動クライアントが、ＧＰＳ又はＰＨＳのローミング機構を用いて自身の現在位置を検出することを特徴とするネットワークアクセスの認証方式。

【請求項８】　請求項６記載のネットワークアクセスの認証方式において、
前記位置情報が、今回のアクセス時における移動クライアントの位置を示す第１の位置情報と、移動クライアントの移動範囲を決めるために設定された第２の位置情報とを含み、
前記アクセス許可手段が、前記第１の位置情報から移動クライアントが前記移動範囲内に存在しないと前記判定手段により判定されたとき、前記アクセスを不正アクセスと判断することを特徴とするネットワークアクセスの認証方式。

【請求項９】　請求項６記載のネットワークアクセスの認証方式において、
前記移動クライアントからのログイン名及びパスワード名と、予め蓄積されるログイン名データ及びパスワード名データとが一致するか否かを確認する手段を更に備え、
前記確認手段から一致した旨の確認結果が得られたとき、前記判定手段及び前記アクセス許可手段の処理動作が実行されることを特徴とするネットワークアクセスの認証方式。

【請求項１０】　移動クライアントがネットワーク上のサーバから所望の情報を取得する環境において、
前記移動クライアントの前記サーバへのアクセス時に、移動クライアントからの位置情報に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可する手段を備えることを特徴とするネットワークアクセスの認証方式における前記移動クライアント、前記サーバ及び前記手段としてコンピュータを動作させるためのコンピュータプログラムを担持したコンピュータ読取可能なプログラム媒体。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、移動クライアント（端末）が、ネットワーク上のサーバから所望の情報を取得する環境に適用されるネットワークアクセスの認証方式に関する。

【０００２】
【従来の技術】移動端末とネットワークサーバとの間の情報通信処理は、通常、移動端末とネットワーク側のリモートアクセスサーバ（アクセスサーバ）との間に設定される専用のプロトコルを利用し、アクセスサーバからの接続許可により、移動端末から移動体通信網を通じた

ネットワークアクセスが可能になった状態で行われる。上記接続許可は、端末携帯者が入力したログイン名及びパスワード名が正当な利用者のものであるとアクセスサーバが認証することにより移動端末に与えられる。専用のプロトコルには、ＰＰＰ（ポイントツーポイントプロトコル）やＳＬＩＰ（シリアルラインインターネットプロトコル）等がある。

【０００３】

【発明が解決しようとする課題】ところで、従来においては、移動端末の携帯者が正当な利用者であるか否かの判断は、予めアクセスサーバ側に判断基準として保存する正当な利用者に係るログイン名データ及びパスワード名データと、移動端末から与えられるログイン名及びパスワード名とを比較し、両者が一致するか否かによって行われていた。そのため、仮に移動端末からのログイン名及びパスワード名が正当な利用者のものであったとしても、アクセスサーバ側では果たして正当な利用者から送信されたものであるか否かを確認することができない。例えば、上記保存されているデータが何らかの原因によって第三者に漏洩した場合に、第三者が正当な利用者になりすましてアクセスサーバにそれらのデータを送信しても、アクセスサーバ側ではそれらをチェックする手段はないから、第三者による不正なネットワークアクセスを容認する結果になってしまう。

【０００４】また、上記保存データが第三者へ漏洩しなかったとしても、不正行為を行おうとする第三者が種々のログイン名及びパスワード名を繰り返し入力することによりアクセス可能なログイン名及びパスワード名の組合わせを取得し、それを用いて不正なネットワークアクセスを行っても、それを防止することは困難である。

【０００５】更に、移動端末が外出先等で盗難に遭い、盗んだ者がその移動端末を用いてネットワークアクセスを行ったような場合や、或いは盗難に遭わないまでも移動端末を複製され、複製者がその移動端末を用いて不正にネットワークアクセスを行った場合にも、それらの不正アクセスを防止することは困難であった。

【０００６】従って本発明の目的は、移動端末から有線ネットワークへのアクセスにおいて、不正アクセスを防止できるようにすることにある。

【０００７】

【課題を解決するための手段】本発明の第１の側面に従うネットワークアクセスの認証方式は、移動クライアントがネットワーク上のサーバから所望の情報を取得する環境に適用されるもので、移動クライアントのサーバへのアクセス時に、移動クライアントからの位置情報に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可する手段を備える。

【０００８】上記構成によれば、移動クライアントのサーバへのアクセス時に、移動クライアントからの位置情報に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可することとしたので、移動端末から有線ネットワークへのアクセスにおいて、不正アクセスを防止できる。

【０００９】本発明の第２の側面に従うネットワークアクセスの認証方式は、移動クライアントがネットワーク上のサーバから所望の情報を取得する環境に適用されるもので、移動クライアントのサーバへのアクセス時に、移動クライアントからの位置情報によりその移動速度を演算する手段と、演算された移動速度に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可する手段とを備える。

【００１０】本発明の第２の側面に係る好適な実施形態では、移動クライアントが、ＧＰＳ又はＰＨＳのローミング機構を用いて自身の現在位置を検出するようになっている。上述した位置情報は、今回のアクセス時における移動クライアントの位置情報と、前回のアクセス時における移動クライアントの位置情報とを含んでおり、アクセス許可手段は、各位置情報から移動速度演算手段によって求められた移動速度が所定の移動速度上限値を超えたとき、今回のアクセスを不正アクセスと判断する。また、上記実施形態では、移動クライアントからのログイン名及びパスワード名と、予め蓄積されるログイン名データ及びパスワード名データとが一致するか否かを判定する手段を更に備えており、判定手段から一致した旨の判定結果が得られたとき、移動速度演算手段及びアクセス許可手段の処理動作が実行されるようになっている。

【００１１】本発明の第３の側面に従うネットワークアクセスの認証方式は、移動クライアントがネットワーク上のサーバから所望の情報を取得する環境に適用されるもので、移動クライアントのサーバへのアクセス時に、移動クライアントからの位置情報により移動クライアントが所定領域内に存在するか否かを判定する手段と、判定された結果に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可する手段とを備える。

【００１２】本発明の第３の側面に係る好適な実施形態では、移動クライアントは、ＧＰＳ又はＰＨＳのローミング機構を用いて自身の現在位置を検出するようになっている。上述した位置情報は、今回のアクセス時における移動クライアントの位置を示す第１の位置情報と、移動クライアントの移動範囲を決めるために設定された第２の位置情報とを含んでおり、アクセス許可手段は、第１の位置情報から移動クライアントが移動範囲内に存在しないと判定手段により判定されたとき、アクセスを不正アクセスと判断する。また、上記実施形態では、移動クライアントからのログイン名及びパスワード名と、予め蓄積されるログイン名データ及びパスワード名データとが一致するか否かを確認する手段を更に備えており、確認手段から一致した旨の確認結果が得られたとき、判定手段及びアクセス許可手段の処理動作が実行される。

【００１３】本発明の第４の側面に従うプログラム媒体は、移動クライアントがネットワーク上のサーバから所望の情報を取得する環境において、移動クライアントのサーバへのアクセス時に、移動クライアントの位置情報に基づいてアクセスの正当性を判断し、正当と認めたときアクセスを許可する手段を備えることを特徴とするネットワークアクセスの認証方式における移動クライアント、サーバ及び手段としてコンピュータを動作させるためのコンピュータプログラムをコンピュータ読取可能に担持する。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【００１５】図１は、本発明の一実施形態に係るネットワークアクセスの認証方式が適用される移動クライアント―サーバシステムの全体構成を示すブロック図である。

【００１６】上記システムは、図１に示すように、移動クライアントである複数のモバイルコンピュータ（移動端末）１１～１ｎと、複数（原理的には少なくとも３機以上）のＧＰＳ（グローバル・ポジショニング・システム）衛星（本実施形態では４機のＧＰＳ衛星を図示）３１～３４と、地上に設置される基地局５とを備える。上記システムは、上記構成に加えて更に、有線ネットワーク（ネットワーク）７と、リモートアクセスサーバ（アクセスサーバ）９と、認証サーバ１１と、ネットワークサーバ（ファイルサーバ）１３と、ファイル１５をも備える。各移動端末１１～１ｎは、その内部構成が同一であるので、以下、移動端末１１のみについて説明し、残りの移動端末１２～１ｎについては説明を省略する。

【００１７】移動端末１１は、基地局５等を有する移動通信網を通じてネットワーク７上のファイルサーバ１３にアクセス（リモートアクセス）して、ファイルサーバ１３との間で通信することにより、ファイルサーバ１３の管理下にあるファイル１５から携帯者が所望する情報（ファイル）を取得するものである。移動端末１１は、送受信部１７１と、ＧＰＳ１９１と、情報処理部２１１とを備える。

【００１８】送受信部１７１は、各ＧＰＳ衛星３１～３４から夫々無線送信されるＧＰＳ情報を受信して、ＧＰＳ１９１に与えると共に、基地局５を通じて無線送信されたファイルサーバ１３からの情報を、情報処理部２１１に与える。送受信部１７１は、また、ＧＰＳ１９１から与えられる移動端末１１の現在位置情報を、情報処理部２１１から与えられる発ＩＤ情報（つまり、移動端末１１の電話番号情報）、ログイン名、パスワード名及び情報提供要求と共に基地局５に無線送信する。

【００１９】ＧＰＳ１９１は、上記各ＧＰＳ情報を送受信部１７１を通じて読込んで、所定の演算処理を行うことによって移動端末１１の現在位置の経度、緯度及び高さを求め、求めた結果を移動端末１１の現在位置情報として、送受信部１７１に出力する。

【００２０】情報処理部２１１は、サーバ１３への情報提供要求（リモートアクセス）の指令や、予め割当てられたログイン名やパスワード名等が携帯者により移動端末１１に入力されると、内蔵する発ＩＤ情報（移動端末１１の電話番号情報）や、ログイン名及びパスワード名等を、情報提供要求と共に送受信部１７１に出力する。情報処理部２１１は、また、上記情報提供要求に応じた携帯者の所望する情報が送受信部１７１を通じて与えられると、それを読込んで所定の処理を施す。

【００２１】基地局５は、ネットワーク７と移動通信網との間のインタフェースとして機能するもので、送受信部１７１から送信された発ＩＤ情報、ログイン名、パスワード名、移動端末１１の現在位置情報及び情報提供要求を受信し、ネットワーク７を通じてサーバ（９～１３）側に送信する。基地局５は、また、サーバ１３から送信された携帯者の所望する情報を受信し、送受信部１７１に無線送信する。

【００２２】アクセスサーバ９は、正当な利用者に係るログイン名データ及びパスワード名データ等を予め判断基準として保存している。アクセスサーバ９は、上記保存しているログイン名データ及びパスワード名データと、移動端末１１との間に設定されるＰＰＰ或いはＳＬＩＰ等の専用のプロトコルを利用してリモートアクセス時に移動端末１１から与えられるログイン名及びパスワード名とを比較する。そして、この比較の結果、両者が一致しているとき移動端末１１の利用者が正当な利用者であると判断し、両者が不一致であれば不正な第三者であると判断する。アクセスサーバ９による判断の結果は、上記発ＩＤ情報及び上記現在位置情報と共にアクセスサーバ９から認証サーバ１１に通知される。

【００２３】本実施形態では、移動端末１１からのリモートアクセス（ネットワークアクセス）を最終的に認証して移動端末１１に対し、ファイルサーバ１３への接続許可を与えるか否かを最終的に決定する権限が、認証サーバ１１に与えられている。

【００２４】即ち、認証サーバ１１は、アクセスサーバ９から正当な利用者である旨の判断結果が通知されたときのみ、今回のアクセス時における移動端末１１の現在位置情報に基づいて所定の演算処理を行うことにより、上記アクセスが正当なアクセスであるか否か（不正アクセスであるか否か）の最終的な判断を実行する。上記アクセスが正当なアクセスであると判断した場合には、移動端末１１に対しファイルサーバ１３への接続許可を与えるが、そうでない場合には、上記接続許可を与えない。なお、アクセスサーバ９から不正な第三者である旨の判断結果が通知されたときは、上記最終判断を実行することなく、ファイルサーバ１３への接続許可を与えない。

【００２５】ファイルサーバ１３は、認証サーバ１１から上記接続許可が与えられたときにのみ、移動端末１１との間で通信を開始し、移動端末１１の永代者が所望する情報をファイル１５から読出し、ネットワーク７及び基地局５を通じて移動端末１１に送信する。

【００２６】図２は、図１に記載した認証サーバ１１の機能構成を示すブロック図である。

【００２７】認証サーバ１１は、図２に示すように、通信情報処理部２３と、認証情報依存部２５と、発ＩＤ処理部２７と、リモートアクセス処理部２９とを備える。

【００２８】通信情報処理部２３は、移動端末１１がリモートアクセスしたことにより、移動端末１１からの発ＩＤを基地局５及びネットワーク７等を通じて受け取り、発ＩＤ処理部２７へ渡す。

【００２９】認証情報保存部２５は、過去における各々の移動端末１１～１ｎのファイルサーバ１３へのアクセス履歴、即ち、アクセスしたときの時刻データｔｉ及びアクセスしたときの位置データ（ｘｉ、ｙｉ）を、各々の移動端末１１～１ｎの発ＩＤ情報毎に保存する。認証情報保存部２５は、また、発ＩＤ処理部２７からの発ＩＤを提示したアクセス履歴取得要求に応じて、上記発ＩＤに対応する移動端末（１１～１ｎのいずれか）のアクセス履歴を発ＩＤ処理部２７に与える。

【００３０】発ＩＤ処理部２７には、移動端末１１の移動速度上限値として、例えば２００ｋｍ／ｈが予め設定されている。発ＩＤ処理部２７は、通信情報処理部２３から与えられた発ＩＤに対応する移動端末（この場合は、移動端末１１）の過去のアクセス履歴、即ち、移動端末１１が前回アクセスしたときの時刻データｔ１、及びアクセスしたときの位置データ（ｘ１、ｙ１）を認証情報保存部２５から取得する。そして、これらの各データと、今回のアクセス時刻データｔ２、及び今回のアクセス時における移動端末１１の現在位置データ（ｘ２、ｙ２）とに基づき、下記の（１）式により移動端末１１の移動速度ｖを求める。

【００３１】

【数１】

$$\text{移動速度 } v = \sqrt{(x_2-x_1)^2 + (y_2-y_1)^2} \Big/ (t_2-t_1) \quad \cdots\cdots \quad (1)$$

発ＩＤ処理部２７は、（１）式により求めた移動速度ｖと、上記移動速度上限値（２００ｋｍ／ｈ）とを比較した結果、ｖ≦移動速度上限値　であれば、正当なアクセスと判定し、一方、ｖ≧移動速度上限値　であれば、現実的な移動速度でないとして不正アクセスと判定する。そして、これらの判定結果を、リモートアクセス処理部２９に与える。

【００３２】リモートアクセス処理部２９は、発ＩＤ処理部２７から正当なアクセスであるとの判定結果が与えられたとき、移動端末１１のファイルサーバ１３へのアクセスを許可し、不正アクセスであるとの判定結果が与えられたとき、上記アクセスを禁止する。なお、発ＩＤ処理部２７が上記発ＩＤに基づいて認証情報保存部２５にアクセス履歴取得要求を行った結果、移動端末１１に係る過去のアクセス履歴がなかった場合、本実施形態では、リモートアクセス処理部２９は正当なアクセスとして取り扱うものとする。

【００３３】次に、図２に示した各部の処理動作について説明する。

【００３４】まず、移動端末１１がネットワーク７にリモートアクセスすることにより、通信処理部２３は、移動端末１１からネットワーク７を通じて送信される発ＩＤを受け取って、発ＩＤ処理部２７に渡す。この発ＩＤを受け取ると、発ＩＤ処理部２７では、移動端末１１の過去のアクセス履歴の取得要求を認証情報保存部２５に対して行う。これに対して、上記過去のアクセス履歴が認証情報保存部２５から与えられると、発ＩＤ処理部２７では、上記過去のアクセス履歴と移動端末１１から与えられる移動端末１１の現在位置情報及びアクセス時刻等から（１）式に基づき、移動端末１１の移動速度ｖを求める。

【００３５】次に、発ＩＤ処理部２７では、上記移動速度ｖが移動速度上限値である２００ｋｍ／ｈを超えているか否かをチェックし、超えていなければ正当なアクセスであるとして、リモートアクセス処理部２９において上記アクセスが許可される。一方、上記移動速度ｖが例えば４００ｋｍ／ｈ等のような日常生活において利用可能な交通手段では不可能な速度となっている場合には、今回のアクセスは不正アクセスであると判断して、リモートアクセス処理部２９において上記アクセスが禁止されることになる。

【００３６】以上説明したように、本発明の一実施形態によれば、アクセスサーバ９において正当なアクセスであると判断された場合であっても、認証サーバ１１において正当なアクセスであると判断されなかった場合には、アクセスの許可が下りない。そのため、従来のような、漏洩や、移動端末の盗難や不正な操作の繰り返し等により入手したログイン名及びパスワード名を用いた第三者による不正なアクセスを防止することが可能である。

【００３７】次に、上述した本発明の一実施形態の変形例について説明する。

【００３８】上述した実施形態では、図２で示した認証情報保存部２５に、過去における各々の移動端末１１～１ｎのファイルサーバ１３へのアクセス履歴のみを、各移動端末１１～１ｎの発ＩＤ情報毎に保存していた。

【００３９】しかし、本変形例では、ログイン名及びパスワード名と共に、各々の携帯者が移動端末１１～１ｎを

利用する地域（エリア）に関する情報、即ち、利用エリア情報｛（ｘｉ、ｙｉ）－（ｘｊ、ｙｊ）｝を、各移動端末１１～１ｎの発ＩＤ情報毎に認証情報保存部２５に保存しておく。そして、移動端末１１のリモートアクセスにより、通信処理部２３が移動端末１１からの発ＩＤを受け取って発ＩＤ処理部２７に渡すと、発ＩＤ処理部２７は、その発ＩＤにより認証情報保存部２５から移動端末１１の利用エリア情報｛（ｘ１、ｙ１）－（ｘ２、ｙ２）｝を取得する。次に、移動端末１１から与えられる移動端末１１の現在位置情報（ｘ３、ｙ３）と、上記利用エリア情報とを比較対照することにより、上記現在位置が上記利用エリア内に含まれるか否かをチェックする。このチェックの結果、含まれていると判定したときには、正当なアクセスであるとして、リモートアクセス処理部２９において上記アクセスが許可される。一方、上記現在位置が含まれていないと判定したときには、今回のアクセスは不正アクセスであるとして、リモートアクセス処理部２９において上記アクセスが禁止されることになる。

【００４０】図３は、本発明の他の実施形態に係る認証サーバの機能構成を示すブロック図である。

【００４１】上述した一実施形態では、各移動端末１１～１ｎのＧＰＳ１９１～１９ｎが各ＧＰＳ衛星３１～３４から個別に与えられるＧＰＳ情報に基づいて、夫々自身の現在位置を検出し、それを現在位置情報として基地局５を通じてサーバ（９～１３）側に送信するように構成されていた。しかし、本実施形態では、ＧＰＳに代えてＰＨＳ（パーソナル・ハンディホーン・システム）を採用することとしたので、各移動端末１１～１ｎの現在位置検出は、例えば上記基地局５に設けた位置情報センタから提供される各移動端末１１～１ｎに関する位置情報サービスを利用して行われることになる。そのため、本実施形態では、認証サーバ１２に新たに位置情報処理部３１を設けたものである。その他各部の構成については、上記一実施形態におけると同様である。

【００４２】位置情報処理部３１は、発ＩＤ処理部２７から発ＩＤが与えられると、その発ＩＤに対応する移動端末（この場合は、移動端末１１）の今回のアクセス時における現在位置情報の提供を位置情報センタに求める。そして、この求めに応じて位置情報センタから移動端末１１の現在位置情報（上述した（ｘ２、ｙ２）又は（ｘ３、ｙ３））が提供されると、これを発ＩＤ処理部２７に与えることになる。以後の処理については、上述した内容と同様である。

【００４３】なお、上述した内容は、あくまで本発明の各実施形態に関するものであって、本発明が上記内容のみに限定されることを意味するものでないのは勿論である。例えば、上記一実施形態に係る構成と、上記一実施形態の変形例に係る構成とを組合わせて用いることも可能である。また、本発明は、ネットワークアクセスの認証以外にも、アクセスする地域に応じてアクセスレベルやサービスレベルを変更するサービスに適用することも可能である。

【００４４】

【発明の効果】以上説明したように、本発明によれば、移動端末から有線ネットワークへのアクセスにおいて、不正アクセスを防止できるようにすることが可能になる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るネットワークアクセスの認証方式が適用される移動クライアント―サーバシステムの全体構成を示すブロック図。

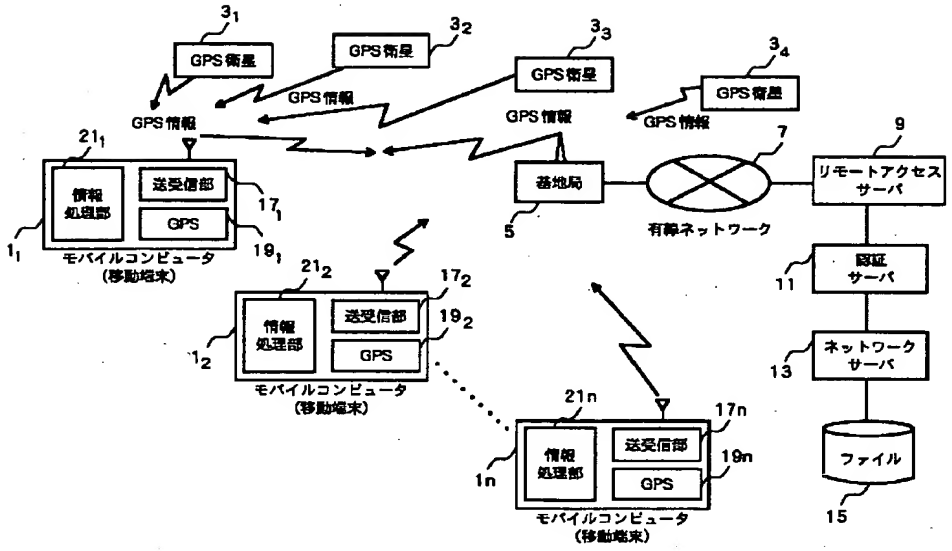
【図２】図１に記載した認証サーバの機能構成を示すブロック図。

【図３】本発明の他の実施形態に係る認証サーバの機能構成を示すブロック図。

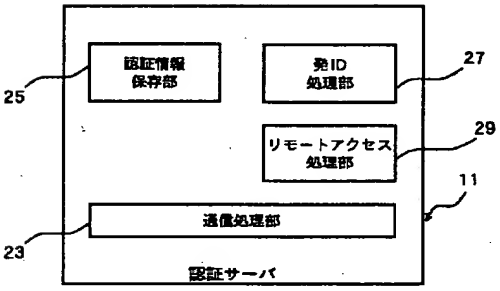
【符号の説明】

１１～１ｎ　モバイルコンピュータ（移動端末）
３１～３３　人工衛星
５　基地局
７　有線ネットワーク
９　リモートアクセスサーバ（アクセスサーバ）
１１　認証サーバ
１３　ネットワークサーバ（ファイルサーバ）
１５　ファイル
１７１～１７ｎ　送受信部
１９１～１９ｎ　ＧＰＳ（グローバル・ポジショニング・システム）
２１１～２１ｎ　情報処理部
２３　通信情報処理部
２５　認証情報依存部
２７　発ＩＤ処理部
２９　リモートアクセス処理部
３１　位置情報処理部

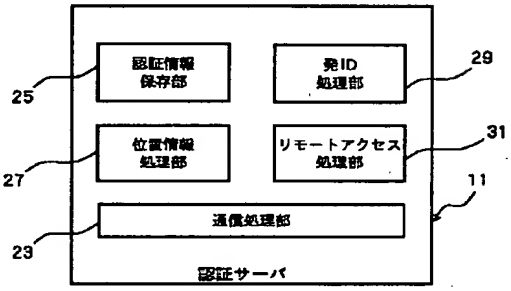
【図１】



【図２】



【図３】



フロントページの続き

Ｆターム(参考)　5B085 AC03 AE01 AE06 AE23 BG07
5K013 AA07 GA00 GA02
5K067 AA32 BB04 BB21 DD17 DD19
DD23 EE02 EE10 GG11 HH22
HH24 JJ52 JJ56